

บทความวิจัย

การประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และสัญญาณ Wi-Fi สำหรับการจัดการระบบรักษาความมั่นคงในที่พักอาศัย

สมพล นิยมแสง¹, ชัยพร เขมะภาตะพันธ์^{2*}วิทยาลัยวิศวกรรมศาสตร์และเทคโนโลยี, มหาวิทยาลัยธุรกิจบัณฑิตย์^{1,2*}อีเมล: 67130088@dpu.ac.th¹, chaiyaporn@dpu.ac.th^{2*}

บทคัดย่อ

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อ 1) นำเสนอวิธีการตรวจจับการบุกรุกในที่พักอาศัยโดยใช้ข้อมูลสถานะช่องสัญญาณจาก Wi-Fi ร่วมกับปัญญาประดิษฐ์และการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติ 2) ศึกษาความทนทานของแบบจำลองเมื่อทำงานข้ามสภาพแวดล้อม 3) ศึกษาตำแหน่งติดตั้งที่เหมาะสมเพื่อลดการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง งานวิจัยเชิงทดลองนี้ใช้ ESP32 เก็บข้อมูล CSI และใช้แบบจำลอง LSTM Autoencoder ที่มีจุดเด่นในการวิเคราะห์ข้อมูลอนุกรมเวลาและเป็นการเรียนรู้แบบไม่มีผู้สอนเพื่อช่วยลดภาระในการติดฉลากข้อมูล และประเมินประสิทธิภาพด้วยค่า Precision, Recall, F1-score และ AUC

ผลการศึกษาพบว่า 1) วิธีการที่นำเสนอมีประสิทธิภาพสูงกว่าแบบจำลองพื้นฐานโดยมีค่า F1-score 0.970 และ AUC 0.995 ในสภาพแวดล้อมเดิม 2) วิธีการที่นำเสนอมีความยืดหยุ่นและทนทานสูงเมื่อทำงานข้ามสภาพแวดล้อมในห้องนั่งเล่นและห้องนอนค่า F1-score 0.933 และ 0.923 ตามลำดับ 3) การแจ้งเตือนผิดพลาดจากสัตว์เลี้ยงลดลงเหลือ 2.41% ที่ความสูง 1.2 เมตร ผลการศึกษาแสดงให้เห็นถึงประสิทธิภาพของวิธีการที่นำเสนอสามารถนำไปประยุกต์ใช้เป็นระบบรักษาความมั่นคงในที่พักอาศัยได้อย่างเป็นรูปธรรม

คำสำคัญ: ไวไฟเซ็นเซอร์, LSTM ออโตเอนโคเดอร์, ตรวจจับการบุกรุก, ข้อมูลสถานะช่องสัญญาณ

Received: 16 April, 2026, **Revised:** 10 May, 2026, **Accepted:** 20 May, 2026

* Corresponding author

APPLICATION OF ARTIFICIAL INTELLIGENCE AND WI-FI SENSING FOR RESIDENTIAL SECURITY MANAGEMENT

Sompol Chimsang¹, Chaiyaporn Khemapatapan^{2*}

College of Engineering and Technology, Dhurakij Pundit University^{1,2*}

Email: 67130088@dpu.ac.th¹, chaiyaporn@dpu.ac.th^{2*}

Abstract

The objectives of this research are: 1) to propose an indoor intrusion detection method for residential areas utilizing Wi-Fi Channel State Information (CSI) integrated with artificial intelligence and an adaptive decision threshold; 2) to investigate the model's robustness in cross-environment operations; 3) to determine the optimal installation position to minimize false alarms triggered by pets. This experimental study employed an ESP32 to collect CSI data and utilized an LSTM Autoencoder model, which excels in time-series data analysis. Its unsupervised learning capability significantly reduces the burden of data labeling. Performance was evaluated using Precision, Recall, F1-score, and AUC.

The results revealed that: 1) the proposed method outperformed the baseline models, achieving an F1-score of 0.970 and an AUC of 0.995 in the original environment; 2) the proposed method demonstrated high flexibility and robustness when operating across environments, achieving F1-scores of 0.933 in the living room and 0.923 in the bedroom, respectively; and 3) false alarms from pets were reduced to 2.41% at an installation height of 1.2 meters. These findings indicate the efficacy of the proposed method, highlighting its practical applicability as a reliable residential security system.

Keywords: Wi-Fi sensing, LSTM Autoencoder, Intrusion Detection, Channel State Information (CSI)

*** Corresponding author**

บทนำ (Introduction)

ปัจจุบัน ปัญหาการบุกรุกและการโจรกรรมในที่พำนักอาศัยเป็นประเด็นสำคัญด้านความมั่นคงปลอดภัยระดับโลก ปัญหานี้ได้สร้างผลกระทบทั่วทุกพื้นที่ทั้งต่างประเทศและในประเทศไทย ผู้ที่ได้รับผลกระทบโดยตรงคือผู้อยู่อาศัยและเจ้าของที่อยู่อาศัย ไม่เพียงต้องเผชิญกับการสูญเสียทางทรัพย์สินแต่ยังรวมถึงความรู้สึกกังวลกับผู้อยู่อาศัย แม้การใช้กล้องวงจรปิดจะเป็นอุปกรณ์มาตรฐานที่ได้รับความนิยมอย่างแพร่หลายแต่ยังคงมีข้อจำกัดด้านความเป็นส่วนตัว โดยเฉพาะการติดตั้งกล้องวงจรปิดในพื้นที่ส่วนตัว เช่น ห้องนอนหรือห้องพักในโรงแรม มักทำให้ผู้อยู่อาศัยเกิดความหวาดระแวง นอกจากนี้ระบบเดิมยังมีข้อจำกัดด้านกายภาพ เช่น ทัศนวิสัยลดลงในที่มืด ความซับซ้อนในการติดตั้ง (Gorrepati, Sahoo, & Udgata, 2023)

เพื่อแก้ปัญหาดังกล่าว เทคโนโลยีการตรวจจับการบุกรุกผ่านสัญญาณไร้สายจึงถูกนำเสนอเพื่อเป็นเทคโนโลยีรักษาความมั่นคงทางเลือก โดยการใช้ข้อมูลสถานะช่องสัญญาณ (Channel state information: CSI) จากสัญญาณ Wi-Fi ที่สามารถสะท้อนการเปลี่ยนแปลงทางกายภาพและการเคลื่อนไหวของมนุษย์ผ่านคุณลักษณะทางฟิสิกส์ของคลื่น วิธีการนี้สามารถตรวจจับการบุกรุกได้โดยไม่ละเมิดความเป็นส่วนตัว (Moghaddam, Shirehjini, & Shirmohammadi, 2022; Ratnam et al., 2024) ในอดีตมีนักวิจัยหลายท่านได้ศึกษาเกี่ยวกับ CSI ร่วมกับเทคโนโลยีปัญญาประดิษฐ์ ตัวอย่าง งานวิจัยของ Gorrepati et al. (2023) ที่ได้นำเสนอระบบตรวจจับการบุกรุกในบ้านผ่านการรับรู้ของสัญญาณ Wi-Fi โดยอาศัยการเรียนรู้ของเครื่องในการจำแนกการบุกรุกในที่พำนักอาศัยซึ่งได้ผลค่า F1-Score สูงถึง 94% นอกจากนี้ในประเทศไทยก็มีการศึกษาดังกล่าว ตัวอย่างเช่นงานวิจัยของ Mekruksavanich and Jitpattanakul (2023) ที่ได้นำเสนอโครงข่ายประสาทเทียมเชิงลึก โดยใช้ชื่อแบบจำลอง CSI-ResNeXt เพื่อใช้ในการจำแนกกิจกรรมในชีวิตประจำวันของมนุษย์ งานวิจัยดังกล่าวได้ทำการศึกษาโดยใช้ชุดข้อมูลสาธารณะมาตรฐาน CSI-HA โดยสามารถให้ผลลัพธ์ค่า F1-Score สูงถึง 99.10% และการพัฒนาระบบตรวจจับการหลอกลวงของ Preechakarnjanadit and Taparugssanagorn (2025) ได้ทำการศึกษาวิเคราะห์ CSI เพื่อสร้างระบบการแจ้งเตือนการหลอกลวงโดยมีการเปรียบเทียบประสิทธิภาพของแบบจำลองการเรียนรู้เชิงลึกสามารถระบุพฤติกรรมการหลอกลวงค่า F1-score สูงถึง 95%

งานวิจัยนี้ได้ทำการศึกษาการประมวลผล CSI ร่วมกับแบบจำลอง LSTM Autoencoder (LSTM AE) เพื่อให้ระบบทำการเรียนรู้ CSI ในสภาวะปกติ (ไม่มีการบุกรุก) เพื่อตรวจจับความผิดปกติหรือมีการบุกรุกของมนุษย์ (Ergen & Kozat, 2020; Khanmohammadi & Azmi, 2024; Mahmoud et al., 2022) การใช้แบบจำลอง LSTM Autoencoder มีจุดเด่นเนื่องจากโครงสร้างถูกออกแบบมาเพื่อจดจำความสัมพันธ์ของข้อมูลอนุกรมเวลาผ่านกระบวนการเข้ารหัส (Encoder) เพื่อบีบอัดและเรียนรู้คุณลักษณะเฉพาะของสัญญาณในสภาวะปกติ และกระบวนการถอดรหัส (Decoder) เพื่อพยายามสร้างสัญญาณนั้นกลับคืนมา ทำให้สามารถวิเคราะห์รูปแบบของคลื่นสัญญาณที่มีการเปลี่ยนแปลงตามเวลาได้ ซึ่งสอดคล้องกับลักษณะของข้อมูล CSI ที่มีความต่อเนื่องและเมื่อมีมนุษย์บุกรุกเข้ามา รูปแบบคลื่นสัญญาณจะเปลี่ยนแปลงไปอย่างฉับพลันทำให้ระบบไม่สามารถสร้างสัญญาณคืนรูปได้เหมือนเดิมและเกิดค่าความคลาดเคลื่อน (Reconstruction Error) ที่สูงขึ้นจนนำไปสู่การแจ้งเตือน ทั้งนี้ เพื่อประเมินประสิทธิภาพอย่างเป็นรูปธรรม งานวิจัยได้ทำการเปรียบเทียบผลลัพธ์กับแบบจำลองพื้นฐานอย่าง Isolation Forest (IF) และ One-class SVM (OCSVM) ซึ่งเป็นแบบจำลองการเรียนรู้แบบไม่มีผู้สอนเช่นเดียวกัน แต่มักมีข้อจำกัดในการวิเคราะห์ความสัมพันธ์เชิงเวลาเมื่อเทียบกับ LSTM

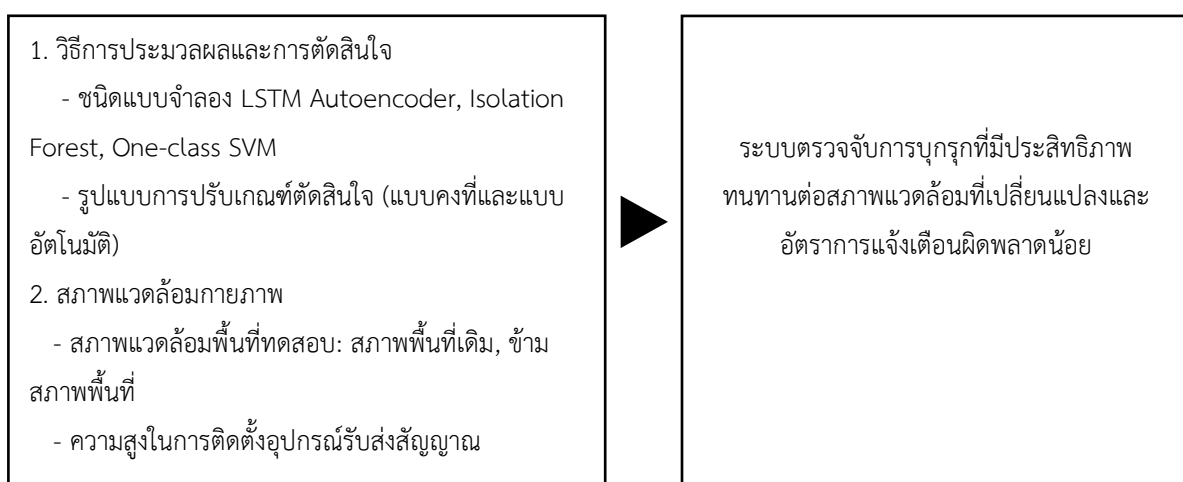
อย่างไรก็ตาม จากการทบทวนวรรณกรรมพบว่า ช่องว่างของงานวิจัยในปัจจุบันคือความเปราะบางของแบบจำลองเมื่อนำไปใช้งานข้ามสภาพแวดล้อมเนื่องจากการเปลี่ยนแปลงทางกายภาพของสภาพแวดล้อมซึ่งส่งผลต่อการกระจายตัวของสัญญาณ ทำให้แบบจำลองที่ใช้การปรับเกณฑ์ตัดสินใจแบบคงที่ (Static Threshold) มีประสิทธิภาพลดลงอย่างรุนแรงและ

จำเป็นต้องเริ่มต้นกระบวนการเรียนรู้ข้อมูลใหม่ทั้งหมด (Jun et al., 2020; Wang et al., 2020) นอกจากนี้ปัญหาการแจ้งเตือนผิดพลาดในกรณีที่มีสัตว์เลี้ยงในที่พักอาศัย ยังคงเป็นอุปสรรคสำคัญที่ลดความน่าเชื่อถือของระบบรักษาความมั่นคงแบบไร้สาย (Lin et al., 2020)

งานวิจัยฉบับนี้จึงนำเสนอวิธีการที่จะปิดช่องว่างดังกล่าวเพื่อให้ระบบตรวจจับการบุกรุกสามารถใช้งานได้จริง โดยการประยุกต์ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติ (Adaptive Threshold) ผ่านการคำนวณค่าเฉลี่ยเคลื่อนที่แบบเอ็กซ์โพเนนเชียล (EMA) (Lee et al., 2022; Wei et al., 2023) และทำงานร่วมกับแบบจำลอง LSTM Autoencoder (Hochreiter & Schmidhuber, 1997) เพื่อปรับปรุงค่า Reconstruction Error (หรือ Loss function) ของ LSTM Autoencoder ตามสถานะสัญญาณรบกวนในสภาพแวดล้อมที่เปลี่ยนแปลงไปในแต่ละช่วงเวลา กลไกดังกล่าวทำให้เส้นเกณฑ์การตัดสินใจสามารถปรับตัวตามแนวโน้มของคลื่นสัญญาณรบกวนพื้นฐานที่มีการเปลี่ยนแปลงตามเวลาในแต่ละพื้นที่ได้อย่างอัตโนมัติ พร้อมทั้งศึกษาตำแหน่งการติดตั้งอุปกรณ์ในระดับความสูงเชิงยุทธศาสตร์ตามทฤษฎีโซนเฟรสนเกลเพื่อแยกแยะการบุกรุกของมนุษย์ออกจากสัตว์เลี้ยง (Lin et al., 2020) โดยในการศึกษานี้ได้กำหนดตัวแปรอิสระ ได้แก่ ชนิดของแบบจำลอง การปรับเกณฑ์ตัดสินใจและเงื่อนไขทางกายภาพของสภาพแวดล้อมในขณะที่ตัวแปรตามได้แก่ประสิทธิภาพการตรวจจับการบุกรุก และอัตราการแจ้งเตือนผิดพลาด โดยอ้างอิงจากงานวิจัยในอดีต (Jun et al., 2020)

เป้าหมายหลักของงานวิจัยนี้ไม่เพียงแต่นำเสนอผลการทดลองทางวิศวกรรมเท่านั้น แต่ยังมุ่งไปถึงการจัดการและการสร้างระบบตรวจจับการบุกรุกที่ทำงานอยู่เบื้องหลัง เพื่อสร้างความมั่นคงให้กับผู้อาศัยโดยไม่ก่อให้เกิดความรู้สึกอึดอัดหรือถูกรบกวนความเป็นส่วนตัวเสมือนถูกเฝ้ามองตลอดเวลา รวมไปถึงลดการแจ้งเตือนผิดพลาดของระบบในกรณีที่มีสัตว์เลี้ยงภายในบ้านที่อาจเพิ่มความเสี่ยงต่อการละเลยต่อเหตุการณ์การบุกรุกจริง งานวิจัยนี้จึงมุ่งหวังที่จะสร้างมาตรฐานใหม่ในระบบรักษาความมั่นคงในที่พักอาศัยและไม่สูญเสียความเป็นส่วนตัว

กรอบแนวคิดการวิจัย (Conceptual Framework)



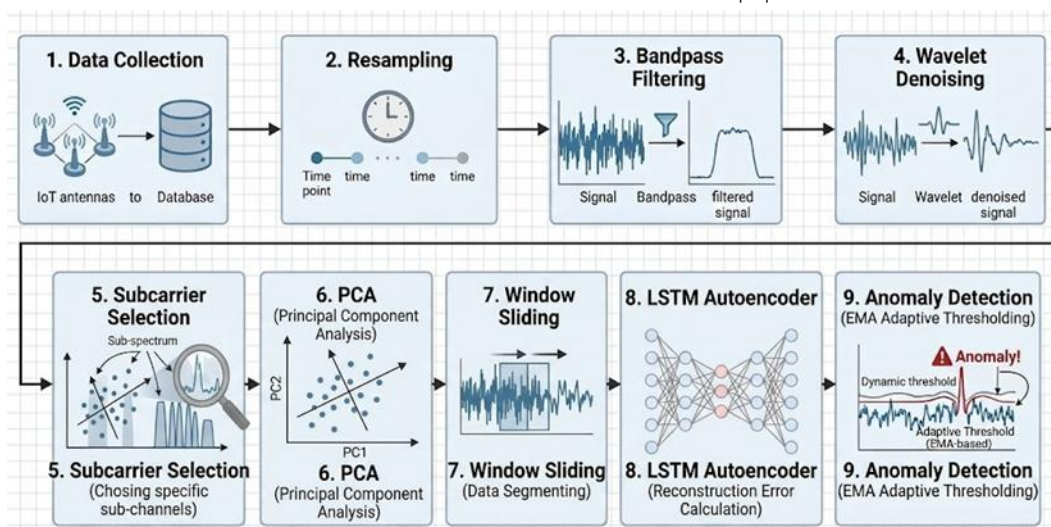
ภาพประกอบที่ 1 กรอบแนวคิดการวิจัย

วัตถุประสงค์ของการวิจัย (Objective of the Research)

1. เพื่อนำเสนอวิธีการตรวจจับการบุกรุกภายในที่พักอาศัยโดยใช้ CSI จาก Wi-Fi ร่วมกับแบบจำลอง LSTM Autoencoder และการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติเพื่อเป็นทางเลือกด้านความมั่นคง
2. เพื่อศึกษาความทนทานของแบบจำลองเมื่อนำไปทดสอบการทำงานข้ามสภาพแวดล้อม
3. เพื่อศึกษาตำแหน่งการติดตั้งอุปกรณ์ตรวจจับการบุกรุกที่เหมาะสม เพื่อลดอัตราการแจ้งเตือนผิดพลาดที่เกิดจากสัตว์เลี้ยง

วิธีวิจัย (Research Methodology)

วิธีดำเนินการวิจัย การวิจัยครั้งนี้เป็นการดำเนินการด้วยวิธีวิจัยเชิงทดลองควบคู่กับการวิจัยเชิงปริมาณโดยมีวัตถุประสงค์หลักเพื่อประเมินประสิทธิภาพจากการประยุกต์ใช้แบบจำลองโครงข่ายประสาทเทียม LSTM Autoencoder ร่วมกับกลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติ ในการตรวจจับความผิดปกติจากการเคลื่อนไหวของมนุษย์ผ่านการวิเคราะห์การเปลี่ยนแปลงตามเวลาของคลื่นสัญญาณ Wi-Fi การทดลองได้ถูกออกแบบเพื่อเปรียบเทียบประสิทธิภาพกับแบบจำลองการเรียนรู้ของเครื่องแบบดั้งเดิมซึ่งเป็นแบบจำลองการเรียนรู้แบบไม่มีผู้สอนเหมือนกันได้แก่ Isolation Forest และ One-Class SVM (Jun et al., 2020; Yong & Brintrup, 2022) เพื่อทดสอบสมมติฐานที่ว่าด้วยการวิเคราะห์ความสัมพันธ์เชิงเวลาที่มีผลต่อความแม่นยำและความทนทานของระบบตรวจจับการบุกรุก



ภาพประกอบที่ 2 แผนภาพสถาปัตยกรรมระบบการตรวจจับการบุกรุกด้วยสัญญาณ Wi-Fi CSI

จากภาพประกอบที่ 2 การประมวลผลแบ่งออกเป็น 9 ขั้นตอน ประกอบด้วย 1) การเก็บรวบรวมข้อมูลด้วย ESP32 เป็นตัวรับส่งสัญญาณ 2) การปรับอัตราสุ่มสัญญาณ (Resampling) 3) การกรองความถี่ด้วยวงจรแถบผ่าน (Band-pass Filter) 4) การลดสัญญาณรบกวนด้วยเวฟเลต (Wavelet denoising) 5) การคัดเลือกคลื่นพาห่อย่อย (Subcarrier selection) 6) การลดมิติข้อมูลด้วยการวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis: PCA) 7) การแบ่งหน้าต่างข้อมูลแบบเลื่อน (Sliding windowing) 8) การประมวลผลด้วยแบบจำลอง LSTM Autoencoder เพื่อคำนวณหาค่าความ

คลาดเคลื่อนจากการสร้างสัญญาณคี่รูป 9) การตรวจจับความผิดปกติ ซึ่งประเมินโดยเปรียบเทียบกับเส้นแบ่งเกณฑ์ปรับตัวที่คำนวณผ่านค่าเฉลี่ยเคลื่อนที่แบบเอ็กซ์โพเนนเชียล เพื่อจำแนกสภาวะปกติและการบุกรุก

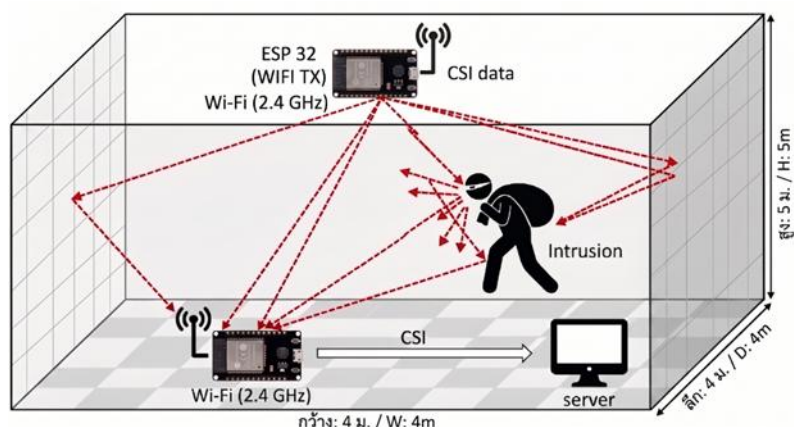
ประชากรและกลุ่มตัวอย่าง ประชากรในการวิจัยนี้คือข้อมูล CSI ที่สะท้อนการเปลี่ยนแปลงสภาพแวดล้อมภายในห้อง โดยกำหนดกลุ่มตัวอย่างด้วยวิธีแบ่งข้อมูลตามช่วงเวลา (Homayouni et al., 2020) เพื่อให้แบบจำลองปัญญาประดิษฐ์สามารถเรียนรู้ความต่อเนื่องของเหตุการณ์และสภาพแวดล้อมโดยกำหนดหน้าต่างเวลาที่ 3.0 วินาที และระยะเลื่อนของเวลา 2.0 วินาที (Moghaddam et al., 2022) โดยทำการจัดเก็บข้อมูลสำหรับการเรียนรู้ของแบบจำลองปัญญาประดิษฐ์ในสภาวะปกติ (ห้องว่าง) เป็นเวลา 120 นาที และชุดข้อมูลทดสอบพฤติกรรมบุกรุกจำนวน 100 เหตุการณ์ต่อสภาพแวดล้อม ซึ่งมีลักษณะเป็นการจำลองเหตุการณ์โดยให้กลุ่มตัวอย่างที่เป็นมนุษย์ทำการเดินหรือเคลื่อนไหวกว้างผ่านพื้นที่ไม่รวมการคลานติดพื้นเพื่อจำลองพฤติกรรมของผู้บุกรุกในสถานการณ์จริง โดยมีข้อกำหนดคือเป็นการตรวจสอบในกรณีที่ไม่มีผู้อยู่ในบ้านเลย (บ้านว่าง) เพื่อป้องกันการแจ้งเตือนผิดพลาดจากการใช้ชีวิตประจำวันตามปกติของผู้อยู่อาศัย ทำให้ได้กลุ่มตัวอย่างทดสอบเชิงสถิติถึง 1,000 หน้าต่างข้อมูลต่อหนึ่งสภาพแวดล้อม (ครอบคลุมทั้งห้องว่าง ห้องนั่งเล่นและห้องนอน)

เครื่องมือวิจัย เครื่องมือวิจัยแบ่งออกเป็น 2 ประเภท

1. ฮาร์ดแวร์สำหรับการรับส่งสัญญาณ บอร์ดไมโครคอนโทรลเลอร์ ESP32 จำนวน 2 ชุด ทำหน้าที่เป็นอุปกรณ์ส่งสัญญาณและรับสัญญาณ (Espressif Systems, 2025) โดยถูกกำหนดให้มีระยะห่างครั้งที่ 4 เมตร และระดับความสูง 1.2 เมตร เพื่อให้เกิดการตัดผ่านเส้นระยะสายตา (Wang et al., 2020) และการทดลองปรับระดับความสูง 0.4 เมตร, 0.8 เมตร และ 1.2 เมตร เพื่อการทดสอบแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง สำหรับแนวทางการยิงวัดระดับนั้น ระบบจะสามารถตรวจพบผู้บุกรุกที่หมอบหรือคลานเข้ามาได้หากพิจารณาเพิ่มการติดตั้งอุปกรณ์รับส่งสัญญาณในระดับต่ำ เช่น 0.4 เมตร ร่วมด้วยหรือพิจารณาการใช้เซ็นเซอร์หลายระดับความสูง ซึ่งจะเป็นแนวทางใหม่ในการแก้ปัญหาและครอบคลุมการตรวจจับในทุกอิริยาบถของผู้บุกรุก

2. ซอฟต์แวร์และแบบจำลอง LSTM Autoencoder โดยกำหนดขนาดชั้นซ่อน 128 โหนด, มิติเวกเตอร์แฝง 16 มิติ (Ergen & Kozat, 2020) อัลกอริทึมพื้นฐานได้แก่ Isolation Forest, One-class SVM (Jun et al., 2020; Yong & Brintrup, 2022) และกลไกเกณฑ์การตัดสินใจแบบปรับตัว ผ่านการคำนวณค่าเฉลี่ยเคลื่อนที่แบบเอ็กซ์โพเนนเชียล (Lee et al., 2022; Wei et al., 2023) การตรวจสอบคุณภาพเครื่องมือ ประเมินความเที่ยงตรง ด้วยการคัดเลือกคลื่นพายุย่อยผ่านดัชนีกิจกรรมเพื่อเลือก 12 ช่องสัญญาณที่ไวต่อการเคลื่อนไหว (Ratnam et al., 2024) และประเมินความเชื่อมั่นด้วยการวิเคราะห์องค์ประกอบหลักเพื่อลดความซ้ำซ้อนเหลือ 8 องค์ประกอบหลัก เพื่อให้ข้อมูลมีเสถียรภาพก่อนเข้าสู่แบบจำลอง LSTM Autoencoder (Moghaddam et al., 2022)

วิธีการเก็บข้อมูลวิจัย



ภาพประกอบที่ 3 สถาปัตยกรรมการจัดวางอุปกรณ์ ESP32 และลักษณะการรวบรวมสัญญาณ CSI เมื่อมีผู้บุกรุก

การจำลองเหตุการณ์ดำเนินขึ้นใน "ห้องปฏิบัติการเสมือนจริง" ภายในที่פקอาศัย โดยติดตั้งฮาร์ดแวร์ ESP32 หน้าเข้าหากันที่ระยะทาง 4 เมตร ดังแสดงในภาพประกอบที่ 2 ระบบจะทำการสุ่มเก็บ CSI ด้วยอัตราการสุ่มตัวอย่าง 1,000 ครั้งต่อวินาที (1 kHz) ซึ่งผลกระทบของช่องสัญญาณที่มีต่อคลื่นลำดับที่ k สามารถอธิบายได้ด้วยสมการเชิงซ้อน ดังนี้

$$H_k = |H_k|e^{j\angle H_k}$$

โดย H_k คือแอมพลิจูด และ $\angle H_k$ คือเฟส ค่าทั้งสองจะเกิดการเปลี่ยนแปลงเมื่อมีการเคลื่อนไหวในสภาพแวดล้อม งานวิจัยฉบับนี้เลือกพิจารณาเฉพาะ "ค่าแอมพลิจูด" เป็นหลักในการประมวลผลเนื่องจากมีคุณสมบัติที่เสถียรและทนทานต่อความคลาดเคลื่อนทางเวลา (Huang et al., 2023) ข้อมูลดิบจะถูกนำมาผ่านกระบวนการกรองความถี่ด้วยวงจรแถบผ่านและการลดสัญญาณรบกวนด้วยเวฟเล็ต ทำการคัดเลือกคลื่นพายุย่อยที่ไวต่อการเคลื่อนไหวผ่านดัชนีกิจกรรม (Ratnam et al., 2024) ดังสมการ

$$AI_k = \left(\int_{0.3}^{3.0} S_k(f) df \right) / \left(\int_{3.0}^{8.0} S_k(f) df \right)$$

โดยที่ $S_k(f)$ คือความหนาแน่นสเปกตรัมกำลัง (Power Spectral Density) ณ ความถี่ f และทำการลดความซ้ำซ้อนของข้อมูลด้วยเทคนิคการลดมิติข้อมูลด้วยการวิเคราะห์องค์ประกอบหลัก (Wang et al., 2022)

ทั้งนี้เพื่อทำการทดลองเกี่ยวกับการแจ้งเตือนผิดพลาดเกี่ยวกับสัตว์เลี้ยงผู้วิจัยได้ทำการทดสอบเชิงทดลองตามทฤษฎีโซนเพรสเนลและความสูงที่มีผลต่อการรบกวนสัญญาณ (Lin et al., 2020) โดยปล่อยสัตว์เลี้ยงขนาดเล็กเดินตัดผ่านเส้นทางการรับส่งสัญญาณในระดับความสูงที่แตกต่างกัน (0.4, 0.8 และ 1.2 เมตร) เพื่อทำการทดสอบการแจ้งเตือนผิดพลาด

สถิติที่ใช้ในงานวิจัย ประกอบด้วย 2 ส่วน

1. การประมวลผลแบบเรียลไทม์ ระบบทำการประมวลผลเพื่อตรวจจับความผิดปกติ (การบุกรุก) โดยใช้แบบจำลอง LSTM Autoencoder และใช้ฟังก์ชันค่าความผิดพลาดยกกำลังสองเฉลี่ยจากความคลาดเคลื่อนระหว่างข้อมูลจริงกับข้อมูลที่แบบจำลองสร้างขึ้นสัญญาณ เพื่อคำนวณคะแนนความผิดปกติ (Mahmoud et al., 2022) ตามสมการ

$$\mathcal{L} = \frac{1}{T} \sum_{t=1}^T ||x_t - \hat{x}_t||_2^2$$

โดยที่ x_t คือข้อมูลจริง และ $\hat{x}_t$ คือข้อมูลที่สร้างขึ้นของแบบจำลอง และ T คือจำนวนจุดข้อมูลภายในหน้าต่างเวลาและอาศัยสถิติพรรณนา ได้แก่ ค่าเฉลี่ย μ_t และส่วนเบี่ยงเบนมาตรฐานของคะแนนความผิดปกติในช่วงเวลาล่าสุด (σ_t) ร่วมกับเทคนิคค่าเฉลี่ยเคลื่อนที่แบบเอ็กซ์โพเนนเชียล (Wei et al., 2023) เพื่อคำนวณเกณฑ์ความผิดปกติเพื่อปรับเปลี่ยนเส้นแบ่งระดับการเตือนภัยอัตโนมัติ ตามสมการ

$$Thresh_t = \mu_t + k \sigma_t$$

โดยที่ k คือพารามิเตอร์สำหรับควบคุมระดับความไว (Sensitivity) ในการแจ้งเตือนเหตุการณ์การบุกรุก

2. การวัดประสิทธิภาพของแบบจำลองเชิงวิชาการ การประเมินประสิทธิภาพของระบบตรวจจัดการบุกรุกด้วยการใช้ Confusion Matrix เพื่อคำนวณตัวชี้วัดประสิทธิภาพได้แก่ ค่าความแม่นยำ (Precision) ค่าความระลึก (Recall) ค่าความสมดุลของการตรวจจับ (F1-score) และการประเมินพื้นที่ใต้โค้งคุณลักษณะ (AUC) เพื่อพิสูจน์ความน่าเชื่อถือของระบบอย่างเป็นรูปธรรม

สรุปผลการวิจัยและอภิปรายผล (Research Conclusions and Discussion)

การประเมินประสิทธิภาพของระบบตรวจจัดการบุกรุกด้วยสัญญาณ Wi-Fi แบ่งการนำเสนอผลการวิจัยออกเป็น 3 ส่วนหลัก ดังนี้

1) การเปรียบเทียบแบบจำลอง LSTM Autoencoder แบบกลไกการปรับเกณฑ์ตัดสินใจแบบคงที่กับแบบจำลองพื้นฐาน

เพื่อประเมินศักยภาพพื้นฐานของแบบจำลองในการตรวจจับความผิดปกติ ผู้วิจัยได้ทำการเปรียบเทียบแบบจำลอง LSTM Autoencoder ที่ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบคงที่กับแบบจำลองพื้นฐานของการเรียนรู้ของเครื่อง ได้แก่ Isolation Forest และ One-Class SVM

ตารางที่ 1 เปรียบเทียบแบบจำลอง LSTM Autoencoder กับแบบจำลองพื้นฐาน

สภาพแวดล้อม	แบบจำลอง	Precision	Recall	F1-score	AUC
ห้องว่าง	LSTM AE	0.984	0.903	0.942	0.995
	IF	0.687	0.986	0.809	0.984
	OCSVM	0.751	0.994	0.855	0.995
ห้องนั่งเล่น	LSTM AE	0.862	0.963	0.910	0.991
	IF	0.321	1.000	0.486	0.970
	OCSVM	0.324	1.000	0.490	0.992
ห้องนอน	LSTM AE	0.990	0.815	0.894	0.992
	IF	0.974	0.852	0.909	0.989
	OCSVM	0.936	0.915	0.925	0.992

จากการทดลองในตารางที่ 1 พบว่า LSTM Autoencoder ให้ประสิทธิภาพเหนือกว่าแบบจำลองพื้นฐานอย่างชัดเจนในสภาพแวดล้อมห้องว่าง โดยมีค่า F1-score 0.942 เมื่อทดสอบข้ามโดเมนในห้องนั่งเล่น ประสิทธิภาพของแบบจำลองพื้นฐานลดลงอย่างรุนแรงต่ำกว่า 0.50 เนื่องจากประจําการเปลี่ยนแปลงและกระจายตัวของสัญญาณรบกวน ในขณะที่ LSTM Autoencoder ยังคงความแม่นยำได้ที่ 0.910 อย่างไรก็ตาม เมื่อทดสอบในห้องนอน ค่า F1-score ลดลงเหลือ 0.894 ซึ่งชี้ให้เห็นถึงข้อจำกัดของการใช้กลไกการปรับเกณฑ์ตัดสินใจแบบคงที่ขาดความยืดหยุ่นในการปรับตัวตามระดับความคลาดเคลื่อนพื้นฐานจากการสร้างกลับข้อมูลของพื้นที่ที่มีสภาพแวดล้อมแตกต่างกัน ทั้งนี้ผลลัพธ์ดังกล่าวแสดงให้เห็นว่าแบบจำลอง LSTM Autoencoder มีประสิทธิภาพในการตรวจจับการบุกรุกสูงกว่าแบบจำลองพื้นฐานถึง 16.44% จากการเปรียบเทียบค่า F1-score ของแบบจำลองพื้นฐานอย่าง Isolation Forest ที่ค่า F1-score 0.809 และแบบจำลองที่นำเสนอ LSTM Autoencoder สามารถทำค่า F1-score สูงถึง 0.942 เป็นเครื่องยืนยันว่า LSTM Autoencoder มีความสามารถในการเรียนรู้และแยกแยะการบุกรุกได้อย่างถูกต้องแม่นยำมากขึ้น

2) การศึกษาความยืดหยุ่นของแบบจำลองเมื่อใช้งานข้ามสภาพแวดล้อม

2.1 การเปรียบเทียบประสิทธิภาพของกลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติและแบบคงที่

เพื่อแก้ไขข้อจำกัดในสภาพแวดล้อมข้ามโดเมน ผู้วิจัยได้ประยุกต์ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติร่วมกับแบบจำลอง LSTM Autoencoder เปรียบเทียบกับการปรับเกณฑ์ตัดสินใจแบบคงที่

ผลการทดลองจาก ตารางที่ 2 แสดงให้เห็นว่าการประยุกต์ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติช่วยยกระดับประสิทธิภาพของแบบจำลอง LSTM Autoencoder ให้เหนือกว่าการปรับเกณฑ์ตัดสินใจแบบคงที่อย่างชัดเจนในทุกสภาพแวดล้อม โดยสามารถเพิ่มค่า F1-score ทั้งในสภาพแวดล้อมการฝึกสอนเดิมห้องว่างจาก 0.942 เป็น 0.970 เพิ่มขึ้น 2.97% ในสภาพแวดล้อมข้ามโดเมนห้องนั่งเล่นจาก 0.910 เป็น 0.933 เพิ่มขึ้น 2.53% และห้องนอนจาก 0.894 เป็น 0.923 เพิ่มขึ้น 3.24% จากผลลัพธ์นี้ยืนยันได้ว่าการประยุกต์ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติ สามารถปรับเปลี่ยนเส้นแบ่งความผิดปกติตามการเปลี่ยนแปลงของสัญญาณรบกวนในแต่ละพื้นที่ได้ ทำให้ระบบสามารถรักษาระดับความแม่นยำในการแยกแยะการบุกรุกเมื่อนำไปใช้งานจริงข้ามสภาพแวดล้อม โดยไม่จำเป็นต้องฝึกสอนแบบจำลองใหม่

ตารางที่ 2 การเปรียบเทียบประสิทธิภาพของกลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติและแบบคงที่

สภาพแวดล้อม	เกณฑ์ตัดสินใจ	Precision	Recall	F1-score	AUC
ห้องว่าง	คงที่	0.984	0.903	0.942	0.995
ห้องนั่งเล่น	คงที่	0.862	0.963	0.910	0.991
ห้องนอน	คงที่	0.990	0.815	0.894	0.992
ห้องว่าง	อัตโนมัติ	0.963	0.977	0.970	0.995
ห้องนั่งเล่น	อัตโนมัติ	0.916	0.950	0.933	0.991
ห้องนอน	อัตโนมัติ	0.963	0.886	0.923	0.992

2.2 การประเมินความสำคัญของกระบวนการย่อย (Ablation Study)

เพื่อประเมินความสำคัญของขั้นตอนการเตรียมข้อมูล ผู้วิจัยได้ทดสอบแบบจำลองโดยตัดบางกระบวนการออกไป โดยเปรียบเทียบกับแบบจำลอง LSTM Autoencoder และการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติ ในกระบวนการปกติซึ่งมีค่า F1-score อยู่ที่ 0.970 (ห้องว่าง), 0.933 (ห้องนั่งเล่น) และ 0.923 (ห้องนอน)

ตารางที่ 3 ผลการทดลองศึกษาการตัดกระบวนการย่อย

สภาพแวดล้อม	ตัดกระบวนการ	Precision	Recall	F1-score	AUC
ห้องว่าง	Wavelet	0.957	0.883	0.919	0.990
ห้องนั่งเล่น	Wavelet	0.963	0.893	0.927	0.990
ห้องนอน	Wavelet	0.970	0.832	0.896	0.983
ห้องว่าง	Selection	0.940	0.937	0.939	0.991
ห้องนั่งเล่น	Selection	0.925	0.923	0.924	0.991
ห้องนอน	Selection	0.937	0.852	0.893	0.980
ห้องว่าง	PCA	0.955	0.974	0.965	0.994
ห้องนั่งเล่น	PCA	0.927	0.940	0.933	0.990
ห้องนอน	PCA	0.956	0.875	0.914	0.991
ห้องว่าง	Bandpass	0.350	1.000	0.518	0.529
ห้องนั่งเล่น	Bandpass	0.320	1.000	0.485	0.522
ห้องนอน	Bandpass	0.301	1.000	0.463	0.370

ผลการทดลองจากตารางที่ 3 ยืนยันว่าทุกขั้นตอนในการประมวลผลสัญญาณล้วนส่งผลต่อประสิทธิภาพการตรวจจับความผิดปกติของแบบจำลองอย่างมีนัยสำคัญเมื่อเทียบกับสถาปัตยกรรมปกติที่ใช้ครบทุกกระบวนการค่า F1-score อยู่ที่ 0.923 - 0.970 สามารถสรุปผลกระทบเมื่อตัดแต่ละขั้นตอนออกได้ดังนี้

1. ผลกระทบรุนแรงที่สุด คือกระบวนการกรองความถี่ด้วยวงจรแถบผ่านเป็นกระบวนการที่ส่งผลกระทบต่อ

แบบจำลองมากที่สุด หากตัดการประมวลผลออกค่า F1-score จะลดลงอย่างรุนแรงเหลือต่ำกว่า 0.52 ในทุกสภาพแวดล้อมซึ่งการประมวลผลการกรองความถี่ด้วยวงจรแถบผ่านคือหัวใจสำคัญในการคัดแยกคลื่นความถี่ของการเคลื่อนไหวออกจากสัญญาณรบกวนภายนอก

2. ผลกระทบระดับปานกลาง คือกระบวนการลดสัญญาณรบกวนด้วยเวฟเล็ตและการคัดเลือกคลื่นพหุย่อยการตัดกระบวนการใดกระบวนการหนึ่งออกทำให้ประสิทธิภาพข้ามโดเมนลดลงเหลือประมาณ 0.89 ซึ่งให้เห็นว่าทั้งสองกระบวนการช่วยรับมือกับสัญญาณรบกวนแบบฉับพลันและรักษาความเสถียรของพื้นที่แฝง (Latent space) ได้ดี

3. ผลกระทบระดับต่ำ คือการลดมิติข้อมูลด้วยการวิเคราะห์องค์ประกอบหลักแม้การตัดออกจะส่งผลทำให้ความแม่นยำลดลงเพียงเล็กน้อย แต่กระบวนการนี้ยังคงจำเป็นต่อการลดรูปความซับซ้อนของข้อมูลช่วยให้แบบจำลอง LSTM Autoencoder เรียนรู้ได้รวดเร็วและมีประสิทธิภาพ

3) การศึกษาตำแหน่งการติดตั้งที่เหมาะสมเพื่อลดการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง

การประเมินความสูงของตัวรับส่งสัญญาณเพื่อลดการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง เพื่อศึกษาผลกระทบของความสูงในการติดตั้งอุปกรณ์รับส่งสัญญาณ ที่มีผลต่อการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง ผู้วิจัยได้ทำการทดสอบจำลองให้สัตว์เลี้ยงเดินผ่านแนวตดขวางตัวส่งและตัวรับสัญญาณเพื่อประเมินการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง โดยงานวิจัยนี้กำหนดขอบเขตของสัตว์เลี้ยงให้หมายถึงสัตว์สี่ขาขนาดเล็กถึงขนาดกลางที่มีความสูงขณะเดินปกติไม่เกิน 0.5 เมตร และมีพฤติกรรมเคลื่อนที่บนพื้นปกติ ไม่ครอบคลุมพฤติกรรมการปีนป่ายหรือกระโดดขึ้นเฟอร์นิเจอร์ ซึ่งอาจทำให้ตัวสัตว์ตัดผ่านระดับความสูงของสัญญาณที่กำหนดไว้

ตารางที่ 4 ผลการทดลองศึกษาความสูงของตัวรับส่งสัญญาณและการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยง

ความสูงของตัวรับส่งสัญญาณ	การแจ้งเตือนผิดพลาด
0.4 เมตร	41.60%
0.8 เมตร	20.40%
1.2 เมตร	2.41%

ผลการทดสอบในตารางที่ 4 ยืนยันสมมติฐานทางทฤษฎีความสูงที่มีผลต่อการรบกวนสัญญาณการติดตั้งอุปกรณ์ที่ระดับความสูง 0.4 เมตร เกิดการแจ้งเตือนผิดพลาดสูงถึง 41.60% แต่เมื่อปรับระดับความสูงของอุปกรณ์ 1.2 เมตร อัตราการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยงจะลดลงอย่างมีนัยสำคัญเหลือเพียง 2.41%

การอภิปรายผล จากการนำเสนอวิธีการตรวจจับการบุกรุกภายในที่พักอาศัยด้วยการใช้ CSI จาก Wi-Fi ร่วมกับแบบจำลอง LSTM Autoencoder เพื่อเป็นเทคโนโลยีทางเลือกในด้านรักษาความมั่นคง ผลการวิจัยชี้ให้เห็นว่าแบบจำลอง LSTM Autoencoder สามารถเรียนรู้การเปลี่ยนแปลงของคลื่นสัญญาณตามเวลาในสภาวะปกติและตรวจจับการบุกรุกได้อย่างแม่นยำ โดยค่า F1-score ในสภาพแวดล้อมเดิมได้สูงถึง 0.970 ซึ่งเหนือกว่าแบบจำลองพื้นฐานอย่าง Isolation Forest และ One-Class SVM อย่างชัดเจน ผลลัพธ์นี้ช่วยสนับสนุนข้อเสนอของ Jun et al. (2020) ที่ระบุว่าแบบจำลองที่ปราศจากการพิจารณาความสัมพันธ์เชิงเวลามักมีความเปราะบางและไม่สามารถจับรูปแบบที่ซับซ้อนของข้อมูลอนุกรมเวลาได้เมื่อเกิดการเปลี่ยนแปลงของการกระจายตัวข้อมูล ทั้งนี้ ผลลัพธ์ของงานวิจัยฉบับนี้สอดคล้องกับงานวิจัยในอดีตดังกล่าว โดยสามารถอธิบายเหตุผลประกอบได้ว่าการประยุกต์ใช้ LSTM ทำให้ระบบสามารถจดจำรูปแบบและการเปลี่ยนแปลงตามเวลาของสัญญาณรบกวนที่สอดคล้องกับพฤติกรรมมนุษย์ได้ดีกว่าแบบจำลองที่ไม่วิเคราะห์ความสัมพันธ์เชิงเวลา

ในการแยกแยะสัตว์เลี้ยงจากการบุกรุกของมนุษย์ ผลการทดลองสอดคล้องกับทฤษฎีโซนเฟรสนелและความสูงที่มีผลต่อการรบกวนสัญญาณ การปรับความสูงตัวรับส่งสัญญาณเป็น 1.2 เมตร ทำให้คลื่นตัดผ่านระดับลำตัวมนุษย์ ในขณะที่สัตว์เลี้ยงมีความสูงทางกายภาพต่ำกว่า จึงเคลื่อนที่อยู่เพียงขอบล่างของโซนคลื่นระดับใต้เส้นระยะสายตาทำให้เกิดสัญญาณแทรกสอดของคลื่นที่มีขนาดเล็กมาก แบบจำลองจึงสามารถแยกแยะความแตกต่างและลดอัตราการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยงลงเหลือเพียง 2.41% ได้อย่างมีประสิทธิภาพ โดยถือเป็นความสอดคล้องกับทฤษฎีคลื่นวิทยุในอดีตที่ว่าระยะความสูงของการตัดผ่านมีผลโดยตรงต่อพื้นที่รับสัญญาณรบกวน

จุดค้นพบที่สำคัญของงานวิจัย คือการแก้ปัญหาข้อจำกัดเมื่อต้องนำระบบไปใช้งานข้ามสภาพแวดล้อมการทดลอง พิสูจน์ให้เห็นว่า การประยุกต์ใช้กลไกการปรับเกณฑ์ตัดสินใจแบบคงที่ทำให้ประสิทธิภาพของแบบจำลองลดลงเมื่อเผชิญกับโครงสร้างทางกายภาพและสภาพแวดล้อมที่แตกต่างจากเดิม การใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติช่วยให้แบบจำลองสามารถประเมินและปรับเกณฑ์การตรวจจับความผิดปกติตามระดับสัญญาณรบกวนพื้นฐานของแต่ละพื้นที่ได้อย่างอัตโนมัติ ทำให้รักษาระดับ F1-score ไว้ได้สูงกว่า 0.92 ในห้องนั่งเล่นและห้องนอน ผลลัพธ์นี้สอดคล้องกับงานวิจัยของ Lee et al. (2022) และ Wei et al. (2023) ที่ยืนยันว่าการใช้กลไกการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติผ่านการคำนวณค่าเฉลี่ยเคลื่อนที่แบบเอ็กซ์โพเนนเชียล สามารถเพิ่มความทนทานต่อการเปลี่ยนแปลงสภาพแวดล้อมได้อย่างมีนัยสำคัญ และยังช่วยลดภาระในขั้นตอนการระบุฉากข้อมูลและไม่จำเป็นต้องฝึกสอนใหม่ ซึ่งถือว่าสอดคล้องอย่างสมบูรณ์กับงานวิจัยก่อนหน้านี้ เนื่องจากวิธีการที่นำเสนอในงานวิจัยนี้สามารถปรับตัวตามการเปลี่ยนแปลงของสัญญาณในแต่ละสภาพแวดล้อมได้แบบอัตโนมัติและจัดการกับข้อจำกัดเรื่องการทำงานข้ามสภาพแวดล้อมได้จริง

นอกจากนี้ ผลจากการประเมินความสำคัญของกระบวนการย่อยยังเป็นข้อพิสูจน์ว่า ขั้นตอนการประมวลผลสัญญาณอย่างเป็นระบบโดยเฉพาะการใช้กระบวนการการกรองความถี่ด้วยวงจรแถบผ่านร่วมกับกระบวนการลดสัญญาณรบกวนด้วยเวฟเล็ตซึ่งเป็นกลไกสำคัญในการลดสัญญาณรบกวนภายนอกและสกัดคุณลักษณะเฉพาะของเวลาที่เกิดจากการเคลื่อนไหวของมนุษย์ ทำให้พื้นที่แฝงของแบบจำลอง LSTM Autoencoder สามารถเรียนรู้และแยกแยะสภาวะปกติและการบุกรุกของมนุษย์ในสภาวะแวดล้อมจริงได้อย่างแม่นยำและน่าเชื่อถือ

สรุปได้ว่า การใช้เทคโนโลยีปัญญาประดิษฐ์ร่วมกับคุณลักษณะทางฟิสิกส์ของคลื่นสัญญาณ Wi-Fi CSI ไม่เพียงยกระดับความแม่นยำในการตรวจจับการบุกรุกและลดอัตราการแจ้งเตือนผิดพลาด ดังตัวเลขสถิติที่แสดงให้เห็นถึงการพัฒนาที่ดีขึ้น คือ สามารถยกระดับค่า F1-score ได้สูงกว่าแบบจำลองพื้นฐานถึงร้อยละ 16.44 และลดการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยงเหลือ 2.41% ทั้งยังเป็นการตอบสนองต่อนโยบายความเป็นส่วนตัวและกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นรูปธรรม เนื่องจากการตรวจจับผ่านคลื่นสัญญาณโดยปราศจากการบันทึกภาพ ช่วยลดความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลของผู้อยู่อาศัย แม้การดำเนินงานจะเกิดขึ้นในที่พักอาศัยตนเองอาจไม่เข้าข่ายความผิดตามกฎหมาย PDPA โดยตรงและอาจไม่สามารถระบุตัวตนของผู้กระทำผิดได้โดยตรงเหมือนกล้องวงจรปิด แต่ระบบได้รับการออกแบบมาเพื่อมุ่งเน้นการตรวจจับและแจ้งเตือนการบุกรุกล่วงหน้า โดยปราศจากการเก็บข้อมูลภาพถ่ายหรือพฤติกรรมส่วนตัวที่อ่อนไหวของเจ้าของบ้านในยามปกติ ซึ่งถือเป็นการตอบสนองนโยบายความเป็นส่วนตัวของเจ้าของบ้านได้อย่างแท้จริง ระบบดังกล่าวสะท้อนให้เห็นถึงกลยุทธ์ใหม่ในการบริหารจัดการระบบรักษาความมั่นคงในสมาร์ตโฮม มีความยืดหยุ่นสูงในการนำไปติดตั้งใช้งานจริงข้ามสภาพแวดล้อม และรักษาความเป็นส่วนตัวได้อย่างมีประสิทธิภาพ

สำหรับข้อจำกัดของการวิจัย แม้ระบบที่นำเสนอจะมีประสิทธิภาพในการทดสอบข้อมูลจำลองการบุกรุก แต่ยังมีข้อจำกัดบางประการ ได้แก่ ข้อจำกัดด้านระยะทางที่ครอบคลุมซึ่งถูกจำกัดไว้ที่ระยะ 4 เมตรภายใต้สภาวะเส้นสายตารวมถึง

ข้อจำกัดของแบนด์วิดท์ของอุปกรณ์ ESP32 ที่อาจไม่สามารถแยกแยะการเคลื่อนไหวที่มีความละเอียดอ่อนมากได้เท่ากับอุปกรณ์รับสัญญาณระดับสูง และข้อจำกัดด้านขอบเขตการตรวจจับในแนวดิ่งแม้การติดตั้งอุปกรณ์ที่ความสูง 1.2 เมตร จะสามารถแก้ปัญหาการแจ้งเตือนผิดพลาดจากสัตว์เลี้ยงได้อย่างมีประสิทธิภาพ แต่ยังเปิดกว้างสำหรับการพัฒนาต่อยอด เพื่อให้ระบบสามารถครอบคลุมการตรวจจับพฤติกรรมในระดับต่ำ เช่น การหมอบหรือคลาน ซึ่งถือเป็นก้าวต่อไปที่สำคัญในการศึกษาและพัฒนาต่อยอดต่อไป

ข้อเสนอแนะ (Suggestion)

ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

1. การขยายขอบเขตการทดสอบในพื้นที่ที่กว้างขึ้นกว่า 4 เมตร หรือในสภาพแวดล้อมที่มีสิ่งกีดขวางซับซ้อน เพื่อประเมินและปรับปรุงความทนทานของแบบจำลองต่อจุดอัปเดตสัญญาณ
2. การศึกษาเพิ่มเติมเกี่ยวกับการจำแนกประเภทการเคลื่อนไหวที่มีความละเอียดอ่อนและซับซ้อนมากขึ้น เช่น การแยกแยะพฤติกรรมการหมอบหรือคลานของผู้บุกรุกออกจากพฤติกรรมของสัตว์เลี้ยง โดยอาจพิจารณาใช้อุปกรณ์ที่มีแบนด์วิดท์สูงขึ้น หรือการติดตั้งเซนเซอร์แบบหลายระดับความสูง
3. ควรมีการศึกษาและประเมินความพึงพอใจจากผู้ใช้งานจริงที่เกี่ยวข้อง (User Satisfaction) เพิ่มเติมเพื่อนำข้อมูลข้อเสนอแนะมาปรับปรุงการทำงานของระบบให้ตอบโจทย์การใช้งานในชีวิตประจำวันมากยิ่งขึ้น

ข้อเสนอแนะสำหรับการนำงานวิจัยไปใช้ประโยชน์

1. ผลการวิจัยนี้สามารถนำไปประยุกต์ใช้ในการพัฒนาระบบรักษาความมั่นคงสำหรับที่พักอาศัย สามารถตรวจจับผู้บุกรุกได้ผ่านสัญญาณ Wi-Fi โดยไม่ต้องติดตั้งกล้องวงจรปิดและการรักษาความเป็นส่วนตัว
2. หลักการปรับเกณฑ์ตัดสินใจแบบอัตโนมัติสามารถนำไปประยุกต์ใช้ร่วมกับระบบเซนเซอร์ IoT ประเภทอื่น ๆ ที่ต้องเผชิญกับสภาวะแวดล้อมที่เปลี่ยนแปลงบ่อย เพื่อยกระดับความแม่นยำในการแจ้งเตือน

เอกสารอ้างอิง (References)

- Ergen, T., & Kozat, S. S. (2020). Unsupervised Anomaly Detection With LSTM Neural Networks. *IEEE Transactions on Neural Networks and Learning Systems*, 31(8), 3127–3141.
- Espressif Systems. (2025). *ESP32-C6-WROOM-1 & ESP32-C6-WROOM-1U Datasheet*. Retrieved from https://documentation.espressif.com/esp32-c6-wroom-1_wroom-1u_datasheet_en.pdf
- Gorrepati, S. R., Sahoo, A. K., & Udgata, S. K. (2023). WiFi Sensing Model for Intrusion Detection in Smart Home Environment. *2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*, pp. 329–334. <https://doi.org/10.1109/R10-HTC57504.2023.10461789>
- Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. *Neural Computation*, 9(8), 1735–1780.
- Homayouni, H., Ghosh, S., Ray, I., Gondalia, S., Duggan, J., & Kahn, M. G. (2020). An Autocorrelation-based LSTM-Autoencoder for Anomaly Detection on Time-Series Data. *2020 IEEE International Conference on Big Data (Big Data)*, pp. 5068–5077. <https://doi.org/10.1109/BigData50022.2020.9378192>

- Huang, J., Liu, B., Miao, C., Lu, Y., Zheng, Q., Wu, Y., Liu, J., Su, L., & Chen, C. W. (2023). Phase Anti: An Anti-Interference WiFi-Based Activity Recognition System Using Interference-Independent Phase Component. *IEEE Transactions on Mobile Computing*, 22(5), 2938–2954.
- Jun, K., Lee, D.-W., Lee, K., Lee, S., & Kim, M. S. (2020). Feature Extraction Using an RNN Autoencoder for Skeleton-Based Abnormal Gait Recognition. *IEEE Access*, 8(1), 19196–19207.
<https://doi.org/10.1109/ACCESS.2020.2967845>
- Khanmohammadi, F., & Azmi, R. (2024). Time-Series Anomaly Detection in Automated Vehicles Using D-CNN-LSTM Autoencoder. *IEEE Transactions on Intelligent Transportation Systems*, 25(8), 9296–9307.
- Lee, S., Jin, H., Nengroo, S. H., Doh, Y., Lee, C., Heo, T., & Har, D. (2022). Smart Metering System Capable of Anomaly Detection by Bi-directional LSTM Autoencoder. *2022 IEEE International Conference on Consumer Electronics (ICCE)*. pp. 1–6. IEEE Consumer Technology Society.
<https://doi.org/10.1109/ICCE53296.2022.9730398>
- Lin, Y., Gao, Y., Li, B., & Dong, W. (2020). Revisiting Indoor Intrusion Detection With WiFi Signals: Do Not Panic Over a Pet! *IEEE Internet of Things Journal*, 7(10), 10437–10449.
- Mahmoud, M., Kasem, M., Abdallah, A., & Kang, H. S. (2022). AE-LSTM: Autoencoder with LSTM-Based Intrusion Detection in IoT. *2022 International Telecommunications Conference (ITC-Egypt)*, pp. 1–6. Air Defense College (ADC).
<https://doi.org/10.1109/ITC-Egypt55520.2022.9855688>
- Mekruksavanich, S., & Jitpattanakul, A. (2023). A Lightweight Deep Residual Network for Recognizing Activities in Daily Living Using Channel State Information. *2023 IEEE 14th International Conference on Software Engineering and Service Science (ICSESS)*, pp. 171–174. Institute of Electrical and Electronics Engineers <https://doi.org/10.1109/ICSESS58500.2023.10293055>
- Moghaddam, M. G., Shirehjini, A. A. N., & Shirmohammadi, S. (2022). A WiFi-based System for Recognizing Fine-grained Multiple-Subject Human Activities. *2022 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, pp. 1–6. IEEE Instrumentation and Measurement Society (IMS). <https://doi.org/10.1109/I2MTC48687.2022.9806622>
- Preechakarnjanadit, D., & Taparugssanagorn, A. (2025). Real-Time, Non-Intrusive Fall Detection via Wi-Fi CSI: A Comparative Study of CNN-LSTM, GNN, and Transformer Models. *AI, Computer Science and Robotics Technology. Intech Open Journals*, 4(1), 1-43.
- Ratnam, V. V., Chen, H., Chang, H.-H., Sehgal, A., & Zhang, J. (2024). Optimal Preprocessing of WiFi CSI for Sensing Applications. *IEEE Transactions on Wireless Communications*, 23(9), 10820–10833.

- Wang, Xiangyu, Wang, X., Mao, S., Zhang, J., Periaswamy, S. C. G., & Patton, J. (2022). Adversarial Deep Learning for Indoor Localization With Channel State Information Tensors. *IEEE Internet of Things Journal*, 9(19), 18182–18194. h
- Wang, Xingang, Wang, Y., & Wang, D. (2020). A Real-time CSI-based Passive Intrusion Detection Method. *2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*. pp. 1091–1098. IEEE Computer Society. <https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00163>
- Wei, Y., Jang-Jaccard, J., Xu, W., Sabrina, F., Camtepe, S., & Boulic, M. (2023). LSTM-Autoencoder-Based Anomaly Detection for Indoor Air Quality Time-Series Data. *IEEE Sensors Journal*, 23(4), 3787–3800.
- Yong, B. X., & Brintrup, A. (2022). Do Autoencoders Need a Bottleneck for Anomaly Detection? *IEEE Access*, 10(1), 78455–78471.